Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2772

Vragen van de leden **Verhoeven** en **Hachchi** (beiden D66) aan de Staatssecretaris van Veiligheid en Justitie, de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie over *het bericht dat kwetsbaarheden in encryptiesoftware door Amerikaanse inlichtingendiensten zijn gebruikt* (ingezonden 2 juni 2015).

Antwoord van Staatssecretaris **Dijkhoff** (Veiligheid en Justitie), mede namens de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie (ontvangen 3 juli 2015). Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 2677

Vraag 1
Kent u het wetenschappelijk artikel over kwetsbaarheden in het Diffie-Hellman-sleuteluitwisselingsprotocol?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening van de wetenschappers dat het zeer aannemelijk is dat de National Security Agency (NSA) via deze kwetsbaarheden toegang heeft verkregen tot VPN- (Virtual Private Network), SSH- (Secure Shell) en TLS (Transport Layer Security) verkeer? Zijn er bij u signalen bekend dat ook inlichtingendiensten van andere landen of niet-statelijke actoren deze kwetsbaarheden hebben gebruikt?

Antwoord 2
Zoals ook aangegeven in de beantwoording op de vragen van het lid Oosenbrug (PvdA) wordt in het wetenschappelijk artikel, naast een uitleg van de Logjam bug, gespeculeerd over de mogelijkheden van de NSA of andere statelijke actoren om als passieve aanvaller (die het internetverkeer tussen een server en een klant uitsluitend registreert en probeert te ontcijferen) het verkeer te kraken. De onderzoekers stellen dat in veelgebruikte communicatie-protocollen (voor beveiligde internetverbindingen, voor geauthentiseerde toegang tot afgeschermde netwerken, of voor mailsystemen) een vercijfer-methode gebruikt wordt die gezien de huidige stand van de techniek niet

[1] https://weakdh.org/imperfect-forward-secrecy.pdf

ah-tk-20142015-2772
ISSN 0921 - 7398
’s-Gravenhage 2015

meer veilig geacht wordt, zeker niet als men bescherming tegen grote statelijke actoren nastreeft.
Inlichtingen- en veiligheidsdiensten geven geen inzicht in de wijze waarop zij hun inlichtingen verzamelen in verband met de bescherming van bronnen, modus operandi en actueel kennisniveau. Om die reden is het niet mogelijk een oordeel te geven of de hypothese van de wetenschappers correct is.
In zijn algemeenheid kan ik u wel aangeven dat, dit in lijn met eerdere adviezen van het NCSC, het van belang is om cryptografische producten op de juiste wijze in te stellen en te gebruiken en dat deze instellingen naar de stand der techniek dienen te worden bezien. Het NCSC heeft reeds eerder geadviseerd om van langere sleutellengtes gebruik te maken dan in het artikel worden genoemd.

Vraag 3, 4, 5 en 6
Bent u van mening dat de Nederlandse overheid toegang zou moeten hebben tot versleutelde data via bestaande kwetsbaarheden of door het (laten) inbouwen van kwetsbaarheden?
Is er sprake van een eenduidig kabinetsbreed beleid ten opzichte van onbekende kwetsbaarheden, oftewel 0-days, of worden in verschillende ministeries verschillende afwegingen gemaakt? Worden alle door de overheid ontdekte, of via het Nationaal Cyber Security Centrum (NCSC) gemelde, 0-days bij de maker van de software gemeld?
Maken defensie, inlichtingendiensten, politie of andere overheidsinstanties ook gebruik van 0-days of alleen van reeds bekende kwetsbaarheden?
Deelt u de mening dat vertrouwen in veilige digitale communicatie en infrastructuur essentieel is voor een goed functionerende digitale economie? Hoe verhoudt zich dat tot een overheid die actief gebruik maakt van kwetsbaarheden in software?

Antwoord 3, 4, 5 en 6
De ingezette acties, zoals gesteld in de Nationale Cyber Security Strategie 2, richten zich op het vinden van een balans tussen veiligheid, vrijheid en economische en maatschappelijke groei. Beveiligde verbindingen en encryptie zijn waardevolle hulpmiddelen voor vertrouwelijke communicatie en opslag van gegevens, met veel gebruiksmogelijkheden. Ook overheden en bedrijven maken gebruik van beveiliging en encryptie om gegevens vertrouwelijk te houden. Het gebruik van adequate beveiliging vermindert de kans slachtoffer te worden van criminaliteit of spionage.
Het kabinet steunt het gebruik van beveiliging en encryptie voor legale doeleinden. Ter versterking van de digitale veiligheid van Nederland en het beperken van de criminaliteit stimuleert het ministerie ook het melden van kwetsbaarheden, onder meer met het beleid voor responsible disclosure.
Ter beantwoording van de resterende vragen verwijs ik u, gezien de overeenkomsten met de door het lid Oostenbrug (PVDA) gestelde vragen, graag naar de in deze bijlage weergegeven antwoorden op de betreffende vragen.
Zoals toegezegd door Minister Kamp in het Algemeen Overleg van 10 juni 2015 inzake de Telecomraad op 12 juni 2015, Den Haag, zal door het kabinet nader worden ingegaan op de thematiek van het gebruik van encryptie.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Oosenbrug (PvdA), ingezonden 27 mei 2015 (vraagnummer 2015Z09552).